NAVAL WAR COLLEGE
Newport, R.I.

The Year 2000 Problem And Its Impact On The CINC; A Way To Mitigate The Impact.

by

William C. Hoppe

Major, United States Army

A Paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

13 February1998

COL Mark A. Kelly, USA,
JMO Faculty Advisor

This Page Intentionally Left Blank

Security Classification This Page is Unclassified

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

The Year 2000 Problem And Its Impact on the CINC; A Way To Mitigate The Impact Damage

9. Personal Authors:
William C. Hoppe, Major, US Army

10.Type of Report: FINAL	11. Date of Report: 13 February 1998

12.Page Count: 33

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Year 2000Problem, Millennium Bug, Y2K Problem, Automation, Operational Logistics

15.Abstract: There is a problem looming on the horizon. Some automated systems are already being affected, others have yet to reach their event horizon. The problem is categorically lumped into the heading; the Year 2000 Problem. The Y2K problem has generated much interest in commercial and government circles. However, the Y2K problem should be generating similar interest and concern in operational circles as well. Like Murphy's Law, the Y2K problem will impact the operational commander. Unlike Murphy's Law, the impact of the Y2K problem *will* be severe. It will degrade the operational commander's ability to plan and execute assigned missions.

Commanders must put in place steps and procedures to ensure operational logistics functions do not totally fail the operational commander. This paper articulates a problem; the impact of the Y2K problem on the operational function of logistics and its impact on the combatant commanders (CINCs) and service component commanders. This paper will explain the magnitude of the problem and most importantly, some techniques and processes that the CINC and service component commanders should implement to mitigate the impact of the problem.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	20.Office Symbol: C

Security Classification of This Page Unclassified

Abstract of

THE YEAR 2000 PROBLEM AND ITS IMPACT ON THE CINC; A WAY TO MITIGATE THE IMPACT.

There is a problem looming on the horizon. Some automated systems are already being affected, others have yet to reach their event horizon. The problem is categorically lumped into the heading; the Year 2000 Problem. The Y2K problem has generated much interest in commercial and government circles. However, the Y2K problem should be generating similar interest and concern in operational circles as well. Like Murphy's Law, the Y2K problem will impact the operational commander. Unlike Murphy's Law, the impact of the Y2K problem *will* be severe. It will degrade the operational commander's ability to plan and execute assigned missions.

Commanders must put in place steps and procedures to ensure operational logistics functions do not totally fail the operational commander. This paper articulates a problem; the impact of the Y2K problem on the operational function of logistics and its impact on the combatant commanders (CINCs) and service component commanders. This paper will explain the magnitude of the problem and most importantly, some techniques and processes that the CINC and service component commanders should implement to mitigate the impact of the problem.

> *"Murphy's Law say, "If it can go wrong, it will go wrong." The logistician acknowledges the real-world wisdom in that law, and responds in two ways. First, he or she tries to keep as many options open as long as possible, even after identifying and pursuing a particular alternative. Second, within the constraints of time and budget, he or she tries to build (just enough) redundancy into the chosen alternative so that a minor oversight, shortfall, human frailty, or mishap won't doom an entire strategy. The logistician doesn't deny Murphy's Law, but instead tries to quarantine its potential impacts."*[1]
>
> —LTG William G. Pagonis
> Commander, 22nd Support Command, Desert Shield/Desert Storm

INTRODUCTION

LTG Pagonis' statement provides some very sound advice for logisticians. It is also very good advice for any organization that has a reliance on information technology. There is a problem looming on the horizon. Some automated systems are already being affected, others have yet to reach their event horizon. The problem is categorically lumped into the heading: The Year 2000 Problem (hereafter referred to as Y2K problem). The Y2K problem has generated much interest in commercial and government circles. However, the Y2K problem should be generating similar interest and concern in operational circles as well. Like Murphy's Law, the Y2K problem will impact the operational commander. Unlike Murphy's Law, the impact of the Y2K problem *will* be severe. It will degrade the operational commander's ability to plan and execute assigned missions. The reason it will have such an effect is our reliance on information technology which has permeated every aspect of operational planning and execution.

There are many aspects of operational planning and execution that the operational commander uses to synchronize operational-level activities. Collectively, these activities are called operational functions. These operational functions are: command and control, intelligence, movement and maneuver, fires, logistics, and protection.[2] Automation has impacted all of the operational functions to some degree. The impact of automation on all these factors does not need explanation to understand the problem. To illustrate the problem the focus of this paper is the operational commander's ability to perform the operational logistics functions of supply, maintenance, transportation, general engineering, health services, and miscellaneous services.[3] These six logistics processes are defined in Joint Pub 4-0 and are heavily reliant on automation. These logistics systems are the cornerstone of Joint Vision 2010's Focused Logistics concept. Failure of these systems, in part or whole, will degrade the operational commander's ability to plan, prepare, and conduct the operational function of logistics.

To mitigate the potential effects of this problem, commanders must put in place steps and procedures to ensure operational logistics functions do not totally fail the operational commander. This paper articulates a problem: the impact of the Y2K problem on the operational function of logistics and its impact on the combatant commanders (CINCs) and service component commanders. This paper will explain the magnitude of the problem and most importantly, some techniques and processes that the CINC and service component commanders should implement to mitigate the impact of the problem.

BACKGROUND

Operational Logistics. The mission of the armed services is articulated in Title 10, United States Code. The 1997 National Military Strategy stipulates that the US Armed Forces are the military instrument for ensuring our Nation's security. "Accordingly, the primary purpose of the US Armed Forces is to deter threats of organized violence against the United States and its interests, and to defeat such threats should deterrence fail."[4] This deterrence is made credible through Armed Forces that are "...trained, equipped, maintained, and deployed primarily to ensure that our Nation is able to defeat aggression against our country and to protect our national interests." [5]

Since the Goldwater-Nichols Department of Defense Reorganization Act of 1986, the responsibility to prepare for this potential fight has rested with the Combatant Commanders, more commonly referred to as CINCs. Whether the mission comes down from the National Command Authority (NCA) as a crisis or is assigned as a mission in the Joint Strategic Capabilities Plan (JSCP), the CINCs have the responsibility to plan for, and if necessary, execute the mission. The logistics burden is shared between the CINCs and the service component commanders:

> "Services, and warfighting commanders handle logistics. The **Joint Staff** and **Services** concentrate on **strategic** logistic matters. **The supported and supporting commanders' logistic staffs** manage both the **strategic** and **operational** logistic issues affecting missions assigned to the combatant commanders (CINCs) in the Joint Strategic Capabilities Plan by the National Command Authorities (NCA) and other such areas as directed by the combatant commander."[6] (emphasis in the original)

In order to support the CINCs execution of their assigned missions, the Goldwater-Nichols Act gave the CINCs directive authority for logistics. Joint Pub 4-0 describes "directive authority for logistics" this way:

> "The exercise of **directive authority for logistics** by a combatant commander includes the authority to issue to subordinate commander directives, including peacetime measures, necessary to ensure the effective execution of approved operations plans, the effectiveness and economy of operation, and the prevention or elimination of unnecessary duplication of facilities and overlapping of functions among the Service component commands.

> **Implementation and execution of logistics functions** remains the responsibility of the Services and the Service component commanders."[7](emphasis in the original)

The services, and their logistics processes therefore, have a direct impact on the CINCs ability to execute their assigned missions. As stated in the first line of Joint Pub 4-0, "Logistics provides the foundation of combat power."[8] Therefore, the ability for logisticians to support operations and operational planning will directly influence the CINCs in their responsibilities.

The trend in the future is not less technology but more technology. Joint Vision 2010 holds that the application of new technologies will transform current operational concepts into new operational concepts. The four new operational concepts are: dominant maneuver, precision engagement, full dimension protection and, focused logistics.

> "Focused logistics will be the fusion of information, logistics, and transportation technologies to provide rapid crisis response, to track and shift assets even while enroute, and to deliver tailored logistics packages and sustainment directly at the strategic, operational, and tactical level of operations."[9]

The CINC as well as the service component commanders will increasingly be affected by the integration of technology on their ability to execute their missions. The National Military Strategy demands that "US forces have the ability to link information, logistics, and transportation technologies together to permit continuous operations by leaner and more agile forces…"[10]

So far this has been a, "So what, I already knew that!" drill. The problem with all this technology is Murphy's Law. Specifically, the problem is Y2K and Murphy's Law. What is this Y2K problem?

The Y2K Problem. The Y2K problem is not one problem but many problems lumped into a convenient heading called Y2K. The essence of the problem stems from the early days of computing when the most expensive part of an automated system was the hardware, specifically the memory.

In the early days of computing, computer programmers had to optimize in every way they could because memory was so expensive. One of many optimization techniques was to use a two digit year field instead of a four digit year field; instead of 1998 they used 98. This technique did save significant amounts of memory and money. A small math problem demonstrates the impact of this optimization. Calculating the age of a person born in 1950 is easy in 1998. The person is 48 years old; 98 minus 50 results in the value 48. However, in the year 2000 the math looks like this; 00 minus 50 results in the value minus 50. This particular issue is the most commonly known problem. It is by no means the only issue and not necessarily the most problematic of the issues lumped under the Y2K umbrella.

Programmers developed numerous optimization tricks and techniques. If the programmer needed a special flag sequence to identify something unusual it was not uncommon to put a special sequence of characters in the date field. One of the more common special dates was '9999'. There was a reasonable expectation that the system would be replaced before reaching the date, 9 September 1999. Unfortunately, some of those systems are still running and even more importantly, all the data generated by these systems is still in use. Each time a non-compliant system accesses it, and makes calculations with it, the result becomes suspect.

The frugal nature of these programmers lead to a more difficult problem. Date time calculations for the Gregorian calendar take into account leap year every seven years—and a leap year every 400 years. This makes the year 2000 a leap year as well. As an optimization trick the entire date algorithm was not always used. There are programmers that did not implement the 'every 400 year' part of the algorithm. Therefore, there is a good chance that systems running on 29 February 2000, a valid date, will calculate an incorrect date, most likely, 1 March 2000.

The list of other optimization techniques and simple oversights goes on. The computer user with no formal programming background will not be aware of the subtle errors lurking in their system until it starts doing funny things (for a more complete list of dates to test see Appendix A). One of the many additional problems is that some systems don't use this calculated date as a date. Instead they use it as a basis for calculation of other information. Starting with a faulty date calculation makes all following calculations bogus. A system not able to recognize that 1 October 1999 is the start of Fiscal Year 2000 may affect the defense appropriations or the monitoring of financial status's within an organization. A lot of accounting actions are done with Julian dates. Some systems will fail when the date 00001 (1 January 2000) or 00060 (29 February 2000) appears.

Scope of the Problem. The overwhelming majority of these systems are managed by the service components or other defense organizations. The end user of these systems are the CINCs. The Defense Information Systems Agency (DISA) has been accumulating data on all the systems in the Department of Defense. That database is called the Defense Integration Support Tool (DIST). The systems in the DIST run the gamut from embedded weapon systems to standard automation systems. Part of what the service components, agencies, and CINCs report is the compliance status with Y2K.

There are three broad categories of compliance reported: hardware, software, and application. The hardware is naturally the platform, the software is for example the operating system of that platform, and the application is the specific program in question. There are three possible answers to the question of compliance; yes, no, and partial. Table 1 shows the service components on the left. Across the top are the number of applications being tracked (#Apps), the number of those applications known as of 20 January 1998 to be non-compliant (No), partially compliant (Partial), compliant (Yes), and the number of systems on which DISA has no data (No Data).

	#Apps	No	Partial	Yes	No Data
Army[11]	1125	244	141	225	515
Air Force[12]	1478	879	469	18	112
Navy[13]	2269	657	305	1184	123
USMC[14]	165	38	50	77	0
Totals	5037	1818	965	1504	750

Table 1. DIST All Active Applications

Of these 5037 service systems being tracked by DISA, there are a number of systems that each of the services have designated as critical. That list is of course a subset of table 1 and the aggregate numbers by service follow in table 2.

	#Apps	No	Partial	Yes	No Data
Army[15]	395	110	71	107	107
Air Force[16]	376	264	108	1	3
Navy[17]	663	151	165	341	6
USMC[18]	150	33	47	70	0
Totals	1434	525	344	449	116

Table 2. DIST Mission Critical Systems

These are the same organizations that support the CINCs. Aside from the number of systems that are only partially compliant and not compliant, there is a frighteningly long list of systems that has no compliance data. This data only reflects the service components. There are other agencies that have significant numbers of systems that support the CINCs. The Defense Logistics Agency (DLA) is one such organization and there systems have a direct impact on operational logistics functions:

	#Apps	No	Partial	Yes	No Data
DLA All Systems[19]	**116**	**6**	**86**	**2**	**22**
DLA Mission Critical[20]	37	0	32	0	5

Table 3. DIST DLA Systems Rollup.

All these systems might "get fixed" before their event horizon occurs. How much confidence should be placed in these systems until they are validated and certified as compliant? "Knowing with confidence where parts or supplies are located, or when and how they will arrive, is the key to the logistician's ability to support operational requirements."[21] The information technology industry, including the military, is notorious for missing delivery dates on systems. The industry average is "86 percent of all applications are delivered either late or never."[22]

HISTORICAL PERSPECTIVE

Operations Desert Shield/Desert Storm. On 2 August 1990, Iraq invaded the neighboring state of Kuwait. On 7 August 1990, President Bush approved the deployment of combat forces to defend the Kingdom of Saudi Arabia from potential invasion.[23] This action started a process which ended in a enormous coalition buildup.

The United States deployed some 560,000 troops, 1,200 tanks, 1,800 warplanes, and 100 warships to the theater of operations during period 7 August 1990 to 5 March 1991.[24] The buildup in the first ninety days was staggering in terms of personnel and equipment transported into the theater. The first ninety days of Desert Shield alone saw a buildup of 1.2 million tons of material.[25]

The ARCENT logistical plan to support the ground offensive called for the establishment of six logistical bases to support the XVIII and VII Corps. ARCENT was responsible for food, bulk fuel, ground ammunitions, port operations, inland cargo transportation, and construction support for all US Forces and for graves registration after a service exceeded its own organic capabilities.[26] There were 258,701 ARCENT, British, and French forces supported by ARCENT for the ground offensive. This included 11,277 tracked vehicles, 47,449 wheeled vehicles, and 1,619 aircraft[27] to be fueled, armed and maintained. "In accordance with joint doctrine and agreements, ARCENT also retained responsibility for much of the theater logistics support of Air Force Component, Central Command (CENTAF) and MARCENT."[28] This equated to 29.6 million meals, 36 million gallons of fuel, and 114.9 thousand tons of ammunition.[29] ARCENT's 22nd Support Command (SUPCOM) was responsible for stocking these bases with enough material and supplies to sustain 60 days of combat operations.[30]

There was a good deal of material and assets provided by the host nation. However, most of the aviation grade fuel, ammunition, and C Class rations (MREs) had to be brought in to the country. This required requisitioning, ordering, tracking, shipping, and management systems throughout the theater and home stations. A good majority of the bulk material was recorded and cataloged with bar code readers.[31] Bar Code readers were just one of many automation tools used in Desert Shield to make logistics processes more efficient.

The global positioning system (GPS) was one of the technology successes in the Gulf War. It is also one of the cornerstone pieces of technology of Joint Vision 2010's Total Asset Visibility (TAV). GPS allows units to know with a great deal of specificity, their location. The capability this provided all personnel in the theater was demonstrated in the consequent issue of 7,509 GPSs within the theater.[32] These were used by combat, combat support (CS) and combat service support (CSS) units. This is important because GPS will fail on 28 August 1999 due to another problem lumped under the Y2K umbrella called "roll-over" (see Annex C).

A major system in the logistics community is called the Commodity Command Standard System (CCSS). This system is run by the Army and is a standard automated wholesale logistics system that supports the Army Materiel Command (AMC) and other Army and DOD organizations. CCSS performs stock control, supply management, cataloging, provisions, procurement, maintenance, security assistance, and financial management for these organizations.[33] According to Congressional reports it is non-compliant.

Change the Dates. What is the point? What would have happened if Operation Desert Shield/Desert Storm had occurred from 7 August 1999 to 4 March 2000 instead of from 7 August 1990 to 5 March 1991? For starters, many of the automated support systems simply would have failed. All the varied GPS units in the Army inventory would fail. If TAV was implemented, it would fail because of its dependence on systems like GPS and CCSS. Many of the automated systems used to requisition and track material would fail. Many of the planning systems to move material and personnel would fail.

What does failure mean? Failure can have many faces. If the results generated by the systems are unreliable the system has failed. What use is a system if the product of that system is suspect? The systems may not 'come up' at all. The application may 'lock up', the operating system may not function properly, the calculations made by the application may be inaccurate. There are many ways to define failure. The bottom line is that the automated way of doing business has been compromised.

IMPACT ON LOGISTICS

What changes? Simply put, the method of operation changes.

A short example using an existing, valid requisition. It is 30 September 1999, which is in FY99. A valid requisition is due out on 10 October 1999; FY00. On 30 September the requisition is due out in 10 days. On 1 October that same requisition is some 99 years over due and may be automatically canceled by some systems as invalid.

The bottom line is that reliance on the automated way of doing business ends and the old stubby pencil and hardcopy requisition method of doing business takes over.

Scope. Since the joint definition of logistics is so broad, there are a lot of potential automated process failures. The transportation of 560,000 people that deployed to the Persian Gulf required the support of USTRANSCOM. The aircraft are scheduled through automated systems. The scheduling of shipping to deploy the heavy divisions is done by automated systems. The air tasking order (ATO) for the strike missions is an automated process. The ATO drives ammunition and fuel requirements which are also controlled by automation systems. The Army's repair parts (Class IX) are managed through automated systems. These systems covered all the repair parts for two full Corps (XVIII and VII Corps in ARCENT). This was roughly 11,277 tracked vehicles, 47,449 wheeled vehicles, and 1,619 aircraft.[34]

A good portion of the 122 million meals served[35] were in the form of Meals Ready to Eat (MREs) and Tray-Rations (T-Rations) ordered from the United States.[36] This same morass of people and equipment use an enormous amount of ammunition. Ammunition was not something the host nation could supply. At the end of the Gulf War there was approximately 250,000 tons[37] of ammunition on the ground in ammunition storage facilities. That ammunition had to be requisitioned, shipped, handled, and managed going into the Kingdom of Saudi Arabia and back to CONUS when the war was over.

Automation touched every aspect of the buildup, execution, and deployment of US forces in Desert Shield and Desert Storm. But, does this mean the whole operation would have come to a complete halt? Absolutely not. What it means is that planners and personnel called upon to execute the mission would have to modify the way they did business; maybe substantially. It means that instead of a build up that took from 7 August 1990 to 24 February 1991, the time schedule may well have been altered or an alternative plan, with alternative force structure may have been executed.

MITIGATION STRATEGIES

Understand the Scope of the Problem. The first step in any decision process is to understand the problem. What is the mission? There is not one problem here but multiple problems. The unfortunate part is that all the problems are lumped under the heading Y2K. Users and customers of the systems must know what the potential affects are on their systems in order to understand the scope of the problem. This implies that they must know what systems affect their ability to do their jobs.

Understanding the details of every potential problem is a technical issue and one not easily mastered. The users (read CINCs) of the automated systems must know the general problem areas and know who to ask in their organizations to find out if the systems in question are certified as compliant. The CINCs do not have to know the technical solution to the problem. CINCs need to know which systems had a problem and more importantly, they need to know with confidence that it has been fixed.

There are four major areas that can be affected by some form of the miscalculation errors, rounding errors, and algorithm errors. For every system there is a hardware platform, an operating systems, applications, and interfaces. Therefore, for every computer out there, four categories of things (at a minimum) must be checked. Failure of any one of the parts may cause the entire systems to function improperly or produce erroneous results.

All four areas must be kept in mind and certified compliant before the overall system can be considered compliant. Given the 5037 applications in table 1 above, there are at least 20,000 things to check. This would not be a daunting task if there was only one item to check in each area. As previously discussed however, there are multiple items in each area to be checked. As of 20 January 1998, the DIST contained 9873 systems. Do the math. This is not a small job.

Triage. The limited resources available to be applied to this problem demand that systems be prioritized. The three most critical constraints are time, money, and people. There simply is not enough time, money (see Annex B), and qualified people around to fix all the systems. This requires the owners of these systems to first, conduct an inventory of all their automation assets, embedded weapon systems, and all other systems that use computer technology.

Triage is defined as, "...the sorting out of patients, as in battle, to determine priority for treatment."[38] Once an inventory of systems has been accomplished, the systems must be prioritized in the order of importance to be certified. This could be a painful process. Table 2 above was a subset of all the systems tracked by DISA. This is by no means all the systems in the DIST database. There are 1434 critical systems being tracked by DISA for the service components. This does not include all the other agencies.

In most cases this triage is the responsibility of the owners of the systems, the service components. It is important for the CINCs to know which systems affect them. The CINCs need to know where those systems have fallen in the service component priority list.

System Verification/Validation/Certification. Current system verification and certification are varied. The whole issue of certifying a system goes to the issue of trust. Does the user have the confidence in the system to trust the answer the system provides? In the case of the CINCs, do they have the confidence in the systems to trust the execution of their crisis or contingency plans? The CINCs must have someone watching the certification of the systems that affect them. The logical choice is the J6 however each of the staff positions is affected and has a interest.

Backup Processes. The CINC and staff are not going to do the scoping, inventorying, triaging, verification and certification of the majority of these systems. They are however going to be impacted by how the system owners have accomplished that mission. Reliance on alternated processes is a good step but as pointed out in the Army Corps Area Support Group (ASG) doctrine, there is a problem:

> "While limited manual backup procedures may be feasible for selected systems, a manual backup system equivalent to the automated one is usually not practical. Hardware and Software redundancy is the best way to compensate for computer interruption or losses due to enemy activities."[39]

What do you do when the problem is the automation system itself? What do you do when there are no other unaffected systems that have the same capability because they are all affected by the same programming error? This is the reason a CINC and staff must look at their own processes to ensure they know where the potential failure is going to occur. They must know what systems are critical to the accomplishment of their mission so they can have alternative methods developed and in place in the event "Murphy" strikes them.

> "Where a mission critical system is not fixed in time, it is essential that a contingency plan be in place. Agencies are to develop such plans in accordance with the government-wide best practices endorsed by the CIO Council. To assure that such planning has occurred for systems in danger of not being repaired on time, we have asked for a summary of the contingency plan for any mission critical system that is reported behind schedule in two consecutive quarterly reports. We will identify and summarize any such plans in future reports to the Congress."[40]

The governmental departments, including the Defense Department, are reporting service component contingency plans to the Office of Management and Budget on a reoccurring bases. How much input do the CINCs have on these contingency plans?

Training. The final step for the CINCs and staffs is to implement the alternative processes. Having the processes in a book that has never been opened until crisis time historically does not work. The common phrase is to train as we will fight. This is not something new because of the Y2K issues. Most Army doctrine manuals require automation intensive processes and the commanders of those units to train for "periodic automation failures."

Age testing some of the systems to determine more precisely the impact of the potential failure is a form of training. There are some systems that lend themselves to age testing. Aging the system can be as simple as changing the date clock. This can also be very dangerous if this is a production system. There are systems that have expiration dates on software that if the system is aged may expire. Controlled, thought through testing is a potential form of training.

WHAT THE NAYSAYERS THINK

There are those that would argue that this Y2K problem is akin to the "chicken little" syndrome. An article in the January 1998 issue of Crosstalk, a well read Air Force periodical, was intitled, "The Year 2000 Farce". The author contended that fixing all these lines of computer code to calculate a four digit date field instead of the standard two digits was a big waste of time. He contended that a simple solution was to write a computer program that would convert the date when used to the proper format and leave the original data alone.[41]

This approach might work on a particular system. It potentially may fix the two digit date issue an a particular system or set of systems. This is the silver bullet approach to the problems. Problems is plural. The phrase Y2K is a catch all phrase for all the date related problems. This argument demonstrates that the magnitude and scope of this problem has not sunk in. The real nature of the problem is not one particular programming error. There are multiple programming errors and oversights that cannot be corrected by inserting a routine that takes a two digit number and converts it to a four digit number. As previously stated, programmers used more than one programming optimization technique when taking their shortcuts. To believe that a single program is going to solve this problem is naïve.

CONCLUSIONS AND RECOMMENDATIONS

Is this a cataclysm about to happen? No, because there are people that are trying to fix the problem. This is not a phenomenon peculiar to the military. The technical solution to all the automation problems however will not be forthcoming prior to 1 January 2000. 1 January 2000 is not the only magic date on the upcoming calendar.

The CINCs, and Service components must place an emphasis on understanding the scope of the problem, the potential impact it will have on their day-to-day operations, and have alternative processes that are unaffected by the automation "failures" that *are* going to occur.

With an 86 percent late or never delivered rate, there are going to be system failures. Some of these failures may be minor, others may be catastrophic. The only way to minimize the impact of such a failure is to plan now. Because of the number of systems involved, the process of system identification and assessment can not be delayed any longer. All systems, regardless of government department ownership must be assessed with respect to the impact on the CINC. Finally, failure to understand the magnitude of the problem, the difficulty in fixing the problem, and the lack of resources to wait until later to address this problem, could be disastrous.

ENDNOTES

[1] William G. Pagonis. Moving Mountains Lessons in Leadership and Logistics from the Gulf War. (Boston: Harvard Business School Press, 1992), 202.

[2] Milan Vego, "On Operational Art (Draft)" (Unpublished Author Articles and Notes, U.S. Naval War College, Newport, RI: 1997), 17.

[3] Joint Chiefs of Staff, Doctrine for Logistic Support of Joint Operations (Joint Pub 4-0) (Washington, DC: 27 January 1995), I-3.

[4] John M. Shalikashvili, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era. (Washington, DC: September 1997), 5.

[5] Ibid.

[6] Joint Chiefs of Staff, Doctrine for Logistic Support of Joint Operations (Joint Pub 4-0) (Washington, DC: 27 January 1995), I-2.

[7] Ibid., vi.

[8] Ibid., I-1.

[9] John M. Shalikashvili. Joint Vision 2010. America's Military: Preparing for Tomorrow. (Washington, DC: July 1996), 24.

[10] John M. Shalikashvili, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era. (Washington, DC: September 1997), 27.

[11] "Department of the Army All Active Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usarmy.doc> 22 Jan 98.

[12] "Department of the Air Force All Active Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usaf.doc> 22 Jan 98.

[13] "Department of the Navy All Active Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usnavy.doc> 22 Jan 98.

[14] "United States Marine Corps All Active Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usmc.doc> 22 Jan 98.

[15] "Department of the Army Mission Critical Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usarmy_m.doc> 22 Jan 98.

[16] "Department of the Air Force Mission Critical Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usaf_m.doc> 22 Jan 98.

[17] "Department of the Navy Mission Critical Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usnavy_m.doc> 22 Jan 98.

[18] "United States Marine Corps Mission Critical Applications" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/usmc_m.doc> 22 Jan 98.

[19] "Defense Logistics Agency" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/dla.doc> 22 Jan 98.

[20] "Defense Logistics Agency" Defense Information Support Tool (DIST). 20 Jan 98. <https://dist.disa.mil/sbu_docs/dla_m.doc> 22 Jan 98.

[21] Department of the Air Force, Logistics (AFDD 40) (Washington, DC: 11 May 1994), 9.

[22] Peter de Jager, "Throwing Down the Year 2000 Gauntlet"; Crosstalk, January 1998, 5.

[23] Frank N. Schubert and Theresa I. Kraus, The Whirlwind War (Washington DC: Government Printing Office, 1995), 49-50.

[24] William G. Pagonis. Moving Mountains Lessons in Leadership and Logistics from the Gulf War. (Boston: Harvard Business School Press, 1992), 11-12.

[25] Ibid., 14.

[26] Department of Defense, Conduct of the Persian Gulf War, Final Report to Congress, (Washington, DC: 1992), 337.

[27] Ibid., 333.

[28] Ibid.

[29] Ibid., 333-334.

[30] Ibid., 336.

[31] William G. Pagonis. Moving Mountains Lessons in Leadership and Logistics from the Gulf War. (Boston: Harvard Business School Press, 1992), 14.

[32] Richard M. Swain, "Lucky War" Third Army in Desert Storm. (Fort Leavenworth: US Army Command and General Staff College Press, 1994), 59.

[33] United States General Accounting Office, Report to the Director, Army Logistics Systems Support Center, LSSC Needs to Confront Significant Year 2000 Issues, (Washington, DC: 1997), 4.

[34] Richard M. Swain, "Lucky War" Third Army in Desert Storm. (Fort Leavenworth: US Army Command and General Staff College Press, 1994), 352, 354.

[35] William G. Pagonis. Moving Mountains Lessons in Leadership and Logistics from the Gulf War. (Boston: Harvard Business School Press, 1992), 1.

[36] Ibid., 114-115.

[37] Ibid., 13.

[38] Stuart Berg Flexner, ed., The Random House Dictionary, Concise Edition, (New York: 1983),923.

[39] Department of the Army, Area Support Group (FM 54-40) (Washington, DC: October 1995), 3-32.

[40] Office of Management and Budget, Progress on Year 2000 Conversion, (Washington, DC: August 15, 1997)

[41] Peter Errington, "The Year 2000 Farce", Crosstalk, January 1998, 25.

BIBLIOGRAPHY

Bachus, Bruce D. < bachubd@hqda.army.mil > "Dates to consider for testing." 15 December 1997. Listserv message <y2karmy@pentagon-hqdadss.army.mil > (15 December 1997).

Browning, Miriam F. "Winning the Year 2000 War." Army RD&A. November—December 1997. 10-12.

Greaney, Kevin J. "The Year 2000 Problem: Catalyst of Cataclysm for Future Information Operations?" Unpublished Research Project, U.S. Army War College, Carlisle Barracks, PA: 1997.

"Defense Logistics Agency All Active Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/dla.doc> (22 January 1998).

"Defense Logistics Agency Mission Critical Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/dla_m.doc> (22 January 1998).

De Jager, Peter. "Throwing Down the Year 2000 Gauntlet." Crosstalk, January 1998. 5.

Department of Defense, Conduct of the Persian Gulf War, Final Report to Congress. Washington, DC: 1992.

"Department of the Air Force All Active Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usaf.doc> (22 January 1998).

"Department of the Air Force Mission Critical Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usaf_m.doc> (22 January 1998).

"Department of the Army All Active Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usarmy.doc> (22 January 1998).

"Department of the Army Mission Critical Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usarmy_m.doc> (22 January 1998).

"Department of the Navy All Active Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usnavy.doc> (22 January 1998).

"Department of the Navy Mission Critical Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usnavy_m.doc> (22 January 1998).

Errington, Peter. "The Year 2000 Farce." Crosstalk. January 1998. 25.

Flexner, Stuart B. ed., The Random House Dictionary. Concise Edition. New York: 1983.

Harames, Paul. "Year 2000 Problem Fixes: Don't Hold Out for a Silver Bullet." Crosstalk, January 1998, 27-29.

Headquarters, Department of the Air Force, Logistics (AFDD 40) Washington, DC: 11 May1994.

Headquarters, Department of the Army, Area Support Group (FM 4-40) Washington, DC: 3 October 1995.

_____. Basic Doctrine Manual for Supply and Storage (FM 10-15, C1) Washington, DC: 12 December 1990.

_____. General Supply in Theaters of Operations (FM 10-27) Washington, DC: 20 April 1993.

Office of Management and Budget, Progress on Year 2000 Conversion. Washington, DC: August 1997.

Martin, Robert A. "The Testing Slant on the Different Types of Y2K Errors." <Unpublished briefing to the Intelligence Community on Year 2000 Testing Workshop, Washington, DC: 23 Jan 1998> <ftp://tso.belvoir.army.mil/pub/y2k/2feb98/ram1a70.ppt> (5 February 1998).

O'Neill, Don. "Software Inspections and the Year 2000 Problem." Crosstalk, January 1998, 17-18.

Pagonis, William G. Moving Mountains Lessons in Leadership and Logistics from the Gulf War. Boston: Harvard Business School Press, 1992.

Reed, Sarah J. "Defense Logistics Agency's Year 2000 Program: Managing Organization-Wide Conversion and Compliance." Crosstalk, January 1998, 11-16.

Reimer, Dennis J. Army Vision 2010. Washington, DC: 1997.

Shalikashvili, John M. Joint Vision 2010. America's Military: Preparing for Tomorrow. Washington, DC: July 1996.

_____. National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, DC: September 1997.

Schubert, Frank N. and Kraus, Theresa L. The Whirlwind War. Washington, DC: Center for Military History, 1994.

Stephens, Chris. "The Air Force and the Year 2000", Crosstalk, January 1998, 3-4.

Swain, Richard M. "Lucky War" Third Army in Desert Storm. Fort Leavenworth: USACGSC Press, 1994.

Tibbetts, John R. "Power Projection Logistics: What Theater Support Unit?" Unpublished Research Paper, School of Advanced Military Studies, U.S. Command and General Staff College, Fort Leavenworth, KS: 1995.

"United States Marine Corps All Active Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usmc.doc> (22 January 1998).

"United States Marine Corps Mission Critical Applications." Defense Information Support Tool (DIST). 20 Jan 1998. <https://dist.disa.mil/sbu_docs/usmc_m.doc> (22 January 1998).

U.S. Congress. House of Representatives. Government Management and Information Subcommittee of the House Government Reform and Oversight Committee, The Progress of Federal Agencies in Avoiding the Year 2000 Software Problem. Hearing before Subcommittee, 24 February 1997.

_____. House of Representatives. Government Management and Information Subcommittee of the House Government Reform and Oversight Committee, Year 2000 Computing Crisis. Hearing before Subcommittee on Government Management, Information and Technology, Committee on Government Reform and Oversight, House of Representatives, 24 February 1997.

_____. House of Representatives. Government Management and Information Subcommittee of the House Government Reform and Oversight Committee, and the Subcommittee on Technology, House Committee on Science, Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium. Hearing before Subcommittee on Government Management, Information and Technology, Committee on Government Reform and Oversight, House of Representatives, 10 July1997.

_____. House of Representatives. Subcommittee of the House Science Committee; and the Government Management, Technology, and Information Subcommittee of the House Government Reform and Oversight Committee, The Year 2000 Computer Problem. Hearing before Subcommittee, 20 March 1997.

U.S. General Accounting Office. Report to the Acting Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort. Washington, DC: 1997.

_____. Report to the Director, Army Logistics Systems Support Center. Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues. Washington, DC: 1997.

_____. Report to Director of the Defense Logistics Agency. Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems. Washington, DC: 1997.

_____. Report to the Secretary of Defense on Battlefield Automation. Software Problems Hinder Development of the Army's Maneuver Control System. Washington, DC: 1997.

_____. Year 2000 Computing Crisis: Essential Government Functions Calls for Agency Action Now. (Washington, DC: 1997)

U.S. Joint Chiefs of Staff. Doctrine for Logistics Support of Joint Operations (Joint Pub 4-0) Washington, DC: 27 January 1995.

Vego, Milan. "On Operational Art (Draft)." Unpublished Author Articles and Notes, U.S. Naval War College, Newport, RI: September 1997.

Voas, Jeffrey. "Certifying Year 2000 'Fixes'", Crosstalk, January 1998, 19-20.

Appendix A

Below is an email to the Army Year 2000 community from the Army Deputy Chief of Staff for Personnel Y2K representative. It highlights only a portion of the event horizon dates and a cryptic reason for why that particular date is significant. Note that the year 2000 is not the end of the story.

From: Bachus, Bruce D., LTC, DAPE[SMTP:BACHUBD@HQDA.ARMY.MIL]
Reply To: Y2KARMY - Forum to Year 2000 Impacts for the U.S. Army
Sent: Monday, December 15, 1997 7:27 PM
To: Y2KARMY@PENTAGON-HQDADSS.ARMY.MIL
Subject: Dates to consider for testing.

"Testing should include a number of critical dates to ensure compliance and no problems occur prior to, on, or after January 1, 2000. The algorithms of systems need to be tested both for forward and backward processing. The most critical future dates that should be considered for testing at this phase include:

* November 2, 1997 - Overflow HP/Apollo Domain OS
* January 1, 1998 - to ensure that the digits "98" do not trigger a red flag, other program subroutine(s), or cause a processing error
* January 1, 1999 - to ensure that the digits "99" do not trigger a red flag, other program subroutine(s), or cause a processing error
* FY2000 for business and industry - Depending on the business the FY could start on March 1, 1999, July 1, 1999 or match the government fiscal year of October 1, 1999.
* August 22, 1999 Overflow of "end of week" rollovers (e.g. GPS)
* September 9, 1999 (9/9/99 or possibly 9999) - to ensure that the digits "99" or "9999" do not trigger a red flag, other program subroutine(s), or cause a processing error
* October 1, 1999 - first day of Fiscal Year 2000
* January 0, 2000 - - to ensure that this date is NOT processed (some applications do have this problem and counts January 0 as the day before the 1st)
* January 1, 2000 - key date in any compliance testing
* January 3, 2000 - first full work day in the new year
* January 10, 2000 - first 9 character date
* February 28, 2000 - to ensure the leap year is being properly accounted for
* February 29, 2000 - to ensure the leap year is being properly accounted for
* February 30, 2000 - - to ensure that this date is NOT processed
* February 31, 2000 - - to ensure that this date is NOT processed
* March 1, 2000 - to ensure date calculations have taken leap year into account
* October 10, 2000 - first 10 character date
* December 31, 2000 - 366th day of the year
* January 1, 2001 - first day in the 21st Century
* January 1, 2001 - Overflow for Tandem systems

* After January 1, 2002 - to ensure no processing errors occur in backward calculations and processing of dates in the 1980s and 1990s at this point in time

* February 29, 2001 - to ensure that this date is NOT processed as a leap year

* February 29, 2004 - to ensure that this date is processed as a leap year

* January 1, 2010 - Overflow ANSI C Library

* September 30, 2034 - Overflow of Unix time function

* January 1, 2037 - Rollover date for NTP systems

* January 19, 2038 - Overflow of Unix systems

* September 18, 2042 - Overflow of IBM System/360

* February 28, 2100 - last day of February - NOT a leap year

Cheers,
LTC Bachus
PS. Compliments of LTC Ylinen, ODCSPER

Appendix B Costs

Like most accounting practices, the cost of something depends on how you want to define the components of the expense. Defining the cost of fixing the Y2K problem is just as convoluted. Depending on how the costs are calculated, estimates to fix the problem world-wide runs the range from $300 billion to $1 trillion.[1] In the United States federal government that range is from $10 to $30 billion.[2] In the summer of 1997, the Army estimated the cost of fixing approximately 400 critical systems at $500 million.[3] This is an exorbitant expense especially in the light that the federal government has authorized no additional funding. The Office of Management and Budget (OMB) issued the policy that within the federal government no new funds will be allocated to the agencies to fix their Y2K problems. This leaves the government and all its agencies with existing dollars to solve the problem.[4] The Department of Defense and subordinate elements guidance reflects the OMB guidance which essentially means that the systems owners are responsible for taking money from their current programs and applying that money toward their Y2K fixes.

[1] Miriam F. Browning, "Winning the Year 2000 War", Army RD&A, November-December 1997, 10.

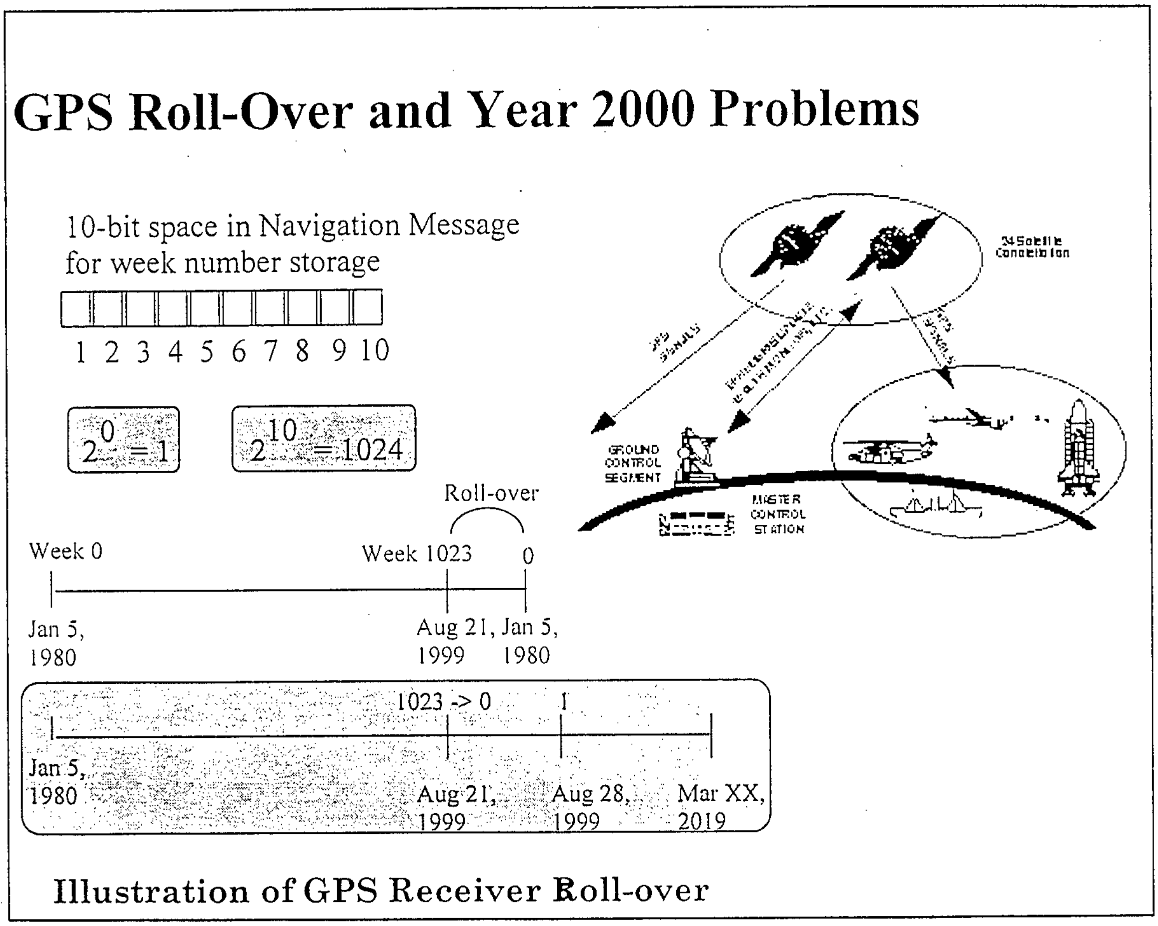
[2] Ibid.

[3] Ibid., 10-11.

[4] Ibid.

Appendix C

The GPS roll-over problem is a hardware problem. The buffer space for storing the value that represents the week is fixed at 10 places. Mathematically that means there are a possible 1024 weeks that can be represented ($2^{10}=1024$). The Initial GPS constellation began operating in January 1980. This means that the week of 21 August 1999 the 10 bit buffer will fill with 1's (1111111111) which will represent the 1024th week. The next week the buffer will "roll-over" to all zeros (0000000000). This date, because of the algorithm, will be calculated as 5 January 1980, not 28 August 1999.



GPS Roll-Over and Year 2000 Problems

10-bit space in Navigation Message
for week number storage

1 2 3 4 5 6 7 8 9 10

$2^0 = 1$

$2^{10} = 1024$

Roll-over

Week 0 — Week 1023 — 0

Jan 5, 1980 — Aug 21, 1999 — Jan 5, 1980

1023 -> 0 — 1

Jan 5, 1980 — Aug 21, 1999 — Aug 28, 1999 — Mar XX, 2019

Illustration of GPS Receiver Roll-over

Figure 1. GPS Roll-Over Slide from The Mitre Corporation briefing on 1/23/1998 to the Intelligence Community Year 2000 Testing Workshop[1]

[1] Robert A. Martin, "The Testing Slant on the Different Types of Y2K Errors" (Unpublished briefing to the Intelligence Community on Year 2000 Testing Workshop, Washington: 23 Jan 1998) <ftp://tso.belvoir.army.mil/pub/y2k/2feb98/ram1a70.ppt>, 5 February 1998.